news release
Senate Select Committee on Intelligence

REPORT OF

THE

SELECT COMMITTEE ON INTELLIGENCE

SUBCOMMITTEE ON SECRECY AND DISCLOSURE

NATIONAL SECURITY SECRETS AND THE

ADMINISTRATION OF JUSTICE

EMBARGO
FOR RELEASE AT 6P.M.
OCT. 10, 1978

October 4, 1978

TABLE OF CONTENTS

I. PREFACE

For more than one year, the Secrecy and Disclosure Subcommittee of the Select Committee on Intelligence has studied the impact of secrecy on the administration of justice in cases involving the national security. During this period, the Subcommittee conducted case studies into investigations and prosecutions where justice has been frustrated by claims of national security.

The Subcommittee discovered that enforcement of laws intended to protect national security information often requires disclosure of the very information the laws seek to protect. Indeed, the more sensitive the information compromised, the more difficult it becomes to enforce the laws that guard our national security. At times then, regardless of whether the compromise is to a newspaper reporter or directly to a foreign agent, the government often must choose between disclosing classified information in a prosecution or letting the conduct go unpunished. In the words of one Justice Department official who testified before the Subcommittee, "To what extent must we harm the national security in order to protect the national security?"

Evidence of this dilemma has been found in investigations not only of leaks and espionage but also of bribery, drug trafficking and murder. Therefore, this dilemma not only adversely affects national security, but also can pervert the administration of justice.

The balance between accountability to the law and protection of national security information is a fragile one. Intelligence agencies through the last several decades have frequently insisted upon the inviolability of the "sources and methods" of intelligence gathering to the exclusion of other concerns. This insistence worked to preclude many prosecutions involving national security information.

In the past three years, however, this imbalance of the past has caused the intelligence community and the Department of Justice to be especially sensitive to the importance of prosecuting such crimes. This administration, much to its credit, has developed ad hoc informal procedures for resolving this dilemma in many cases.

This Committee desires with the appropriate Executive Branch agencies to develop permanent and formal procedures to insure that consideration of the national security should not in itself defeat the principle of accountability. Of course, the Committee is especially concerned that the provisions of the proposed intelligence community charters (S. 2525), which provide for criminal sanctions for egregious intrusions on the rights of Americans, as well as amendments to the espionage statutes intended to protect the identity of our intelligence agents, be enforceable to the fullest extent possible. If the balance in national security cases

in future administrations is skewed once again in favor of the protection of "sources and methods" and other classified information, charter provisions may become unenforceable.

The Committee recognizes the need to confront the issue of whether a major recasting of the existing espionage statutes is or is not necessary. The Committee has nonetheless found that many practical, legal, and political differences and difficulties lie in the path of such an undertaking. Major advances can in the meantime be made in procedures and practices under current statutes that will permit the resolution of many of the dilemmas regarding the use of national security information in the administration of justice.

Although continuing examination of alternatives to the current statutory scheme is necessary, the Committee at this time wishes to recommend certain ameliorative steps, short of any major immediate recasting of the law, because they can yield effective improvement. By contrast, any substantial revision of current statutes will occasion months, if not years, of delay, with no improvement in the meantime.

Furthermore, some of the cases reviewed and testimony received indicate that even the most radical revision of the espionage statutes along the lines of the British Official Secrets Act may not resolve this dilemma. Only the establishment of a secret trial system for these kinds of cases would

resolve the problem described in this report--not in our opinion a very desirable or likely development. Ultimately, the Congress must decide whether leaks of some national security information and the exposure of some such information in prosecutions are the inevitable cost of constitutional guarantees of freedom of speech and the press and the constitutional right to a public trial.

Joseph R. Biden, Jr., Chairman
Subcommittee on Secrecy
and Disclosure

James Pearson, Vice Chairman
Subcommittee on Secrecy
and Disclosure

II. SUMMARY

The Committee's inquiry has led it to the following conclusions:

(A) There has been a major failure on the part of the government to take action in leak cases. To date, we have been unable to identify a single successful prosecution of an individual who leaked information to a publication. Admittedly, the question of whether some leaks are punishable under existing statutes is not altogether clear. The Committee found that leak cases are uniquely difficult to investigate. But, we found cases where no action was taken -- investigation or prosecution -- even where a leak clearly violated an existing statute and caused serious harm to our national security.

The failure has resulted in part from an impasse between the Department of Justice and the intelligence community on how to deal with the futher use of classified information necessary for investigation and prosecution of these leak cases. Briefly stated, there is no effective and formal mechanism for investigating these cases or, in the few cases where the source of the leak is discovered, weighing the risks of additional disclosures against the benefits of prosecution.

(B) Several immediate steps may be taken to facilitate the administration of existing laws, while Congress determines the need for major revision of the espionage statutes. Furthermore,

it is possible that improvements in the administration of existing statutes might affect ultimate decisions on statutory revision. Present day reality and historical precedent show that numerous political and practical obstacles would seriously delay any major new statutes designed to deter leaks. While there is a wide divergence of views among Committee members about what changes, if any, should be made in the espionage statutes, a narrowly drawn provision that would punish disclosure of the identity of American intelligence agents appears to be necessary. For the time being, the Committee has recommended several steps to ensure the removal of obstacles to prosecutions which exist under current law.

(C) Disagreements over the use of classified information in prosecutions also impede espionage prosecutions.

(1) The Committee reviewed some espionage cases which have not proceeded to either investigation or prosecution for the same reason that leak cases cannot proceed -- concern about the disclosure of intelligence information in the course of investigation or prosecution. Furthermore, certain cases engendered such intense disagreements between the intelligence community and the Department of Justice that Presidential intervention to resolve the disagreement was almost required.

(2) However, a resolution of the disagreement over the use of classified information in espionage prosecutions is likely for the following reasons:

(a) Espionage cases are generally considered more serious than leak cases.

(b) The federal espionage statutes are more clearly drawn to cover espionage than most leaks.

(c) Many espionage cases are in effect out of the control of the intelligence community because the law enforcement machinery has been engaged by an arrest, or because the public or officials outside the intelligence community know of the crime and, therefore, pressure the intelligence community to provide information necessary for prosecution.

(d) Usually the constitutional problems (primarily First Amendment problems) are much less severe in espionage cases than in leak cases.

(D) The impasse over the use of classified information in prosecutions occurs in other types of criminal cases and at times defendants may have placed the Department of Justice at a marked disadvantage in perjury, narcotics, and possibly even one murder case.

The Committee has formulated a series of recommendations designed to alleviate some of the problems faced by the government in maintaining the secrecy of legitimate national security information. These recommendations can be found on pages .

III. BACKGROUND OF SECRECY AND DISCLOSURE SUBCOMMITTEE INQUIRY

On April 26, 1977, with the agreement of the full Committee, the Subcommittee on Secrecy and Disclosure asked the staff to undertake (1) a review of unauthorized disclosures of intelligence information and (2) an inquiry into the use of compartmentation -- a procedure to place special limitations on access to information that is especially sensitive. Although some progress has been made on the second inquiry, most of the Subcommittee's work has concentrated on the first question which will serve as the focus of this report.

The Subcommittee conducted its inquiry through both interviews and file searches at the intelligence agencies. Over thirty interviews and briefings were conducted with officials of the Departments of Justice and State and the major intelligence agencies (the Central Intelligence Agency, the National Security Agency, and the Defense Intelligence Agency). In the course of these briefings each agency was asked to provide the Subcommittee with ten cases in which intelligence information had been covertly passed to foreign powers -- classical espionage cases -- or in which intelligence found its way into the public media -- intentional or accidental leak cases. We have reviewed over thirty case files or summaries of case files provided by these agencies. These files have served as a valuable data base for our survey. They represent the most comprehensive compilation of such information

in either the Executive branch or Congress. Each file contains information on an intelligence compromise which has occurred in the last few years, the action taken -- or not taken, as is frequently the case -- by the relevant agency or the FBI, and any disciplinary action taken against the individuals responsible.

In June of last year, after reviewing a summary of the results of its survey, and based on a number of surprising findings, the Subcommittee redirected its inquiry. The Subcommittee originally began on the assumption that the major issue to be addressed would be evaluating the desirability of additional criminal sanctions for unauthorized disclosure of information that jeopardized sensitive foreign intelligence "sources and methods". As the work proceeded, however, the Subcommittee was soon driven to the conclusion that no present statute can be effectively enforced against "leaks" and that it would be a difficult task to draft a constitutional criminal statute which would solve the enforcement problems. In fact, the nation's strictest statutory safeguard against unauthorized disclosure, Section 798 of Title 18, the U.S. espionage statute which protects communications intelligence "sources and methods" in a manner similar to that of the British Official Secrets Act, has been infrequently used despite the large number of leaks of communications intelligence. The files which the Subcommittee has studied reveal several cases in which violations of even this statute were neither investigated nor prosecuted.*

---

* Part of the reason for the reluctance to bring cases under Section 798 is the lack of agreement as to whether courts will require the prosecution to establish the propriety of classification. If a court should decide to look behind the classification of a document, then this would require the public disclosure of additional sensitive information.

At the heart of this failure of enforcement is a very deep-seated conflict between the concerns of the intelligence community on the one hand, and the Department of Justice on the other in enforcing the espionage statutes. The conflict arises over whether publicly to disclose classified information necessary to conduct the investigation and to proceed with the prosecution.* Indeed this question of whether or which classified information is to be used in a particular judicial proceeding is a pervasive problem that goes well beyond enforcement of the espionage statutes. Problems created by classified information have also hampered many other prosecutions, including perjury, extortion, bribery, narcotics violations and possibly even one murder case.

On March 1st, 2nd and 6th, the Subcommittee on Secrecy and Disclosure conducted public hearings on the matters raised by our inquiry. The Subcommittee heard from Admiral Stansfield Turner, the Director of Central Intelligence; Benjamin Civiletti, then the Acting Deputy Attorney General; Philip Lacovara, formerly of the Watergate Special Prosecutor's Office; Judge Albert Fletcher, Chief Judge of the Court of Military Appeals; William Colby, former Director of Central Intelligence; Lawrence Houston, former CIA

---

* It is common knowledge that the FBI and other counterintelligence agencies do from time to time decide not to prosecute espionage cases for other reasons such as the desirability of monitoring a particular spy in order to understand the full dimensions of a spy network. This report does not address these kinds of cases but only those where investigation and prosecution is the preferred approach.

General Counsel; and Morton Halperin, representing the American Civil Liberties Union. The purpose of this report is to summarize the Committee's findings based on these hearings and its year-long inquriy, and to report its recommendations for legislative and administrative actions to facilitate administration of certain statutes related to the national security.

IV. "LEAK" AND CLASSICAL ESPIONAGE INVESTIGATIONS

A. "Leak" Investigations

The Subcommittee examined thirty recent cases submitted by the CIA, NSA and DIA. These cases consisted primarily of instances of leaks of intelligence information to the newspapers. Of those thirty cases only three were actually referred to the Department of Justice for investigation and none of those was formally investigated. All were recent cases. Almost half of the cases involved disclosure of communications intelligence, which could have been prosecuted under Section 798 of Title 18 of the United States Code (see Appendix). As noted earlier, Section 798 is the only espionage provision currently on the books that approaches the strict liability criminal standard used by the British in the Official Secrets Act, the model for recent proposals to create new criminal sanctions for "leaks."

Many of the "leak" cases have not been investigated by the FBI because of the Department of Justice's policy of refusing to investigate unless the intelligence community is willing to declassify all information related to the case. This policy grew out of frustration by the Department over the years with intelligence community reluctance to provide necessary evidence to prosecute major leak cases after the FBI had invested considerable time and effort in investigation.

According to those cases examined by the Subcommittee, the response to those leaks which are subject to internal intelligence agency investigations begins with an employee of an intelligence agency who is familiar with the intelligence and who identifies the possible leak when it is published. For example, if the intelligence relates to information gleaned from communications intelligence, an employee of the unit which processes that intelligence would probably recognize the sensitivity of the published information and report it to the office of security of his agency. Upon receipt of the published article containing the leak, the office of security of the concerned intelligence agency would next attempt to determine the individuals or offices who had access to the information.

This type of investigation is often fruitless because the leaked information has been disseminated broadly in such inter-agency classified materials as certain CIA intelligence cables, the National Intelligence Daily or the Weapons Intelligence Summary (some of which have circulation in the thousands). The very information which must be disseminated to policymakers is frequently the information which requires the greatest protection from unauthorized disclosure. At the same time that the security office is attempting to determine the scope of dissemination and the possible recipients of the information, it is working closely with the office within the intelligence agency where the

information originated in the preparation of a damage assessment.*

After the damage assessment is completed and a cursory review of the number of people who might have had access is finished, the information is forwarded to one of three organizations: to the Security Committee of the Intelligence Community Staff, to another agency if it is clear that the information must have been leaked in a publication or from an office or individuals of that agency, or (in a small fraction of the cases) to the Department of Justice.

If reference to the Department of Justice is indicated, the Department's response is pro forma. According to the cases examined, the Department of Justice does not usually initiate an investigation. It normally responds with a letter back to the agency containing what is called "the eleven questions" (see Appendix). Neither the Department of Justice nor the FBI will normally proceed further until the eleven questions are answered. Some of the eleven questions are uncontroversial -- such as whether the compromised information was properly classified

---

* Most of the damage assessments that were reviewed were quite perfunctory in nature and provided no specific information on the actual and specific damage caused by the leak.
In fairness to those preparing the damage assessment at such an early date in the process, it is difficult to assess the damage because it is not yet clear whether or not a hostile power has actually responded to the information in the article. However, damage assessments were rarely updated in the cases which were reviewed.

in the first place and whether the article disclosing it was accurate. In most cases, particularly those of extreme sensitivity, however, the whole process reaches an impasse at Question 9, which reads as follows:

> Whether the data can be declassified for the purpose of prosecution and, if so, the name of the person competent to testify concerning the declassification.

The intelligence agencies view this as a requirement that they agree to declassify any and all information in question before the Department of Justice will agree to investigate the case. Since the agencies rarely agree to this "up front" commitment, few cases, if any, are ever actually investigated by the Department of Justice. Indeed, of the 30 cases provided by the intelligence agencies, none was investigated by the Department of Justice.

B. Espionage Investigations

Espionage cases -- secretly passing classified information to a hostile power -- are taken much more seriously than leaks by both the Justice Department and the intelligence community. (See discussion on page 44.) Despite the fact that espionage cases and "leaks" may both be prosecuted under the same criminal statutes, the eleven question leak questionnaire is not used in espionage cases. Indeed in espionage cases a resolution is almost always reached between the intelligence community and the Justice Department on how to proceed with investigation. Although the government is capable of resolving its differences

in espionage cases, the decision in the past was often not to prosecute. Recently, the CIA Office of General Counsel and the Criminal Division of the Justice Department have -- much to their credit -- succeeded in surmounting the many obstacles to prosecution in espionage cases. Therefore the initial impasse that prevents the opening of investigations in leak cases does not occur. Nevertheless, even if the decision is to proceed to trial in an espionage case, it is often a painful and hotly contested matter causing friction between the Justice Department and the intelligence community from the grand jury proceedings through sentencing. The Subcommittee examined cases that did proceed to prosecution and one case which was subsequently dropped with no punitive action taken against an individual who admitted to espionage; in that case the individual was granted immunity in return for a full confession of what information he had passed to a foreign nation.

United States v. Moore was the successful prosecution last year of a former CIA official who tossed classified documents onto the Russian Embassy lawn here in Washington. United States v. Boyce and Lee, also successfully prosecuted last year, involves an employee of TRW, a large defense contractor in California, who passed photographs of documents describing extremely sensitive intelligence systems to the Russians. Both cases were the subject of considerable tension between the CIA and the Department of Justice. Both required protracted negotiations on whether to use individual documents and witnesses in the trial. In the Moore case disagreements between DCI George Bush and Attorney General Levi almost required President Ford's intervention on his last day in office.

C. Damage by Confirmation Versus Augmentation

The intelligence agencies' concern about the effect of investigation or prosecution of a leak or classical espionage upon the national security falls into two basic categories:

(1) The investigation or prosecution of an espionage violation can further damage the national security by confirming the validity of the information disclosed. For example, in either a covert transmission case or a leak case a hostile power which discovers information very sensitive to the national security may discount the information because of questions about the reliability of the source, whether it be a spy or a newspaper.

However, if an indictment is filed against the subject or the existence of an investigation is disclosed, the hostile intelligence service might tend to interpret that indictment or investigation as confirmation of the accuracy of the information provided. This particular form of damage to the national security is practically impossible to remedy because of the constitutional requirement of a "public" trial -- the defendant has a right to a public adjudication of the charges against him. This is one reason why criminal sanctions for even the most serious "leaks" to newspapers would be a particularly counter-productive remedy.

(2) Investigation or prosecution may augment the damage to the national security by disclosing either to the defendant or other interested parties further information necessary either to investigate the case or to prove the case. For example, it frequently becomes necessary in the course of investigation to discuss the facts of the case with a variety of witnesses who may be associates of the defendant. In a criminal case there is a plethora of procedures which involve public discussion of evidence related to the crime. This may be particularly risky in espionage cases where prosecution may disclose sophisticated counter-espionage techniques.

D. Augmentation of the Damage in Criminal Cases

This latter problem, augmentation of the damage, may be easier to resolve than the former. Where the Justice Department

has determined to proceed, for example as in the Rosenberg or Ellsberg case, or in the two major espionage prosecutions last year, the prosecutors and judges have fashioned ad hoc procedures to protect the national security and at the same time ensure the administration of justice. These ad hoc procedures form the focus of the Committee's present efforts.

In a criminal prosecution involving perjury, narcotics smuggling, organized crime offenses such as extortion, or espionage, there are a variety of circumstances in the course of pre-trial or trial procedures in which government attorneys fear a judge will require disclosure of classified information.

(1) As part of the case against the defendant. In a typical espionage prosecution, classified information may be directly relevant in proving the case against the defendant. For example, in a prosecution under Section 793 of Title 18, it is necessary to prove that the information passed will actually damage the national security or be of aid to a foreign government. Of course, in some cases the information passed is not of obvious significance to a foreign government and there is always the likelihood the foreign government does not understand the impact of the information passed. In such a criminal trial it becomes necessary to explain to the jury, and therefore to the public and to the intended recipient, the significance of the information passed. For example, in the Moore case the government had to disclose publicly classified information

contained in the documents tossed onto the Embassy lawn, but which in fact were never examined by the Russians.* Thus, here the prosecution could have done as much damage to the national security as the consummated crime.

The Boyce and Lee prosecution earlier this year was one of the very few prosecutions under Section 798 of Title 18 for the unauthorized dissemination of communications intelligence. Even though Section 798 on its face does not require proof of harm, Boyce and Lee were also charged under other sections of the criminal code. Thus, it was necessary to prove that the information was appropriately classified.

(2) As a part of the defendant's affirmative defense. In the course of any of these prosecutions it is likely that the defendant will raise an affirmative defense that will require classified information. For example, an agency official prosecuted for deceiving Congress, might offer the affirmative defense that it was a pattern or practice of Agency officials either to conceal classified information in Congressional briefings or even to deceive Congressional committees. In the alternative, the official might argue that the information he provided the Committee was indeed truthful. Obviously both of these offers of proof would have required the disclosure of a considerable amount of extremely sensitive, classified information. In a

---

* In this case the Federal judge took the extraordinary step of sealing a public trial exhibit (consisting of the directory and other sensitive documents), permitting only limited access by the jury.

case of organized crime and narcotics smuggling, a defendant might allege that a former association with the Agency provides a putative affirmative defense which would require evidence of the CIA's relationship to him or similar agency relationships to other individuals in the underworld.

(3) As part of pre-trial discovery. In every criminal trial the defendant is entitled under the Constitution, under statute, or under the Federal Rules of Criminal Procedure*, to: (a) all materials obtained from or belonging to the defendant; (b) anything "material to the preparation of his defense"; (c) information pertaining to the testimony of a government witness; and, (d) any exculpatory information within the government's possession. Frequently the information which must be disclosed in these pre-trial procedures is classified.

E. "Gray Mail": The Price of Failing To Resolve the Dilemma

Since the Espionage Act was enacted in 1917, the Federal Government has been cautious in using the statute because of the necessity to provide further classified information in the course of a prosecution. Prosecutors in the Department of Justice and intelligence community officials have always recognized that the espionage statute is not an effective remedy for all "leaks" to the newspaper or covert transmission to a foreign spy because of the counter-productive disclosure of further

---

* Rule 16.

secrets. The Department of Justice is also aware that a defense counsel, in the course of trial or through pre-trial discovery, can threaten the government with discovery motions or a line of questioning that requires the disclosure of classified information. An internal CIA study of this problem in 1966 characterizes the dilemma as follows:

> Out of this evidentiary difficulty has come a sort of "gray mail", granted on the immunity from prosecution (and often civil suit as well) enjoyed by the thief who limits his trade to information too sensitive to be revealed.

So long as there is a real threat that prosecution of the defendant may reveal sensitive information in the course of a trial, he or she may engage in this "gray mail" to avoid prosecution.*

---

* Philip Lacovara characterized this problem in particularly strong language.

> ...Agent 007, had a license to kill, but I think the testimony and the findings of the Subcommittee staff...support the judgment that the situation in real life is even more sweeping than Ian Fleming wrote of in his fictional novels...People... connected with intelligence information, whether they are themselves intelligence officers or otherwise involved with national security operations, have by virtue of the immunity from prosecution something like a license not only to kill, but to lie, steal, cheat, and spy...

V. CASES OF "GRAY MAIL"

The ambiguity of the statutes described in previous sections and the internal Executive branch procedures for their enforcement have at times created a legal vacuum -- often tantamount to immunity -- for people who gain access to secret information. The dilemma is most often confronted in the leak and espionage circumstances described earlier, but occurs as well in cases not usually associated with the national security -- bribery, extortion, obstruction of justice or murder.*

The following are actual cases in the public record where secrecy and concerns about disclosure of sources and methods actually interfered with the investigation or prosecution of a serious felony which was not directly related to the national security. These cases are important because they represent not only the different kinds of crimes which give rise to this phenomenon but also the subtlety with which concern about sources and methods can interfere with the administration of justice.

A. A Case of Bribery

In his book The American Black Chamber published in 1933, Herbert Yardley, who directed the United States' first signals

---

* There are no examples of leaks or espionage cases halted for national security reasons included below because any further public discussion of these cases might raise the same concerns as investigations or prosecutions -- further disclosure of legitimate national secrets.

intelligence operation, describes an incident concerning a message which he intercepted between a foreign Ambassador in Washington and his home government. The message implicated the Ambassador in bribery of a high American government official and his secretary.

In a subsequent meeting with a high official in the State Department, Yardley admitted having sent the message to the Attorney General. The State Department official and the Secretary were furious that the Attorney General knew the contents of the intercept even though it pertained to serious criminal activity by government officials.

Yardley had thought it appropriate to send this message over because it looked to him like a Justice Department case. The State Department official was adamant. "The activity of an Ambassador is never a Justice Department case," he stated.

Yardley himself warned that if the Ambassador were recalled, "His government will appoint a new ambassador, install a new code, and one never knows how much difficulty a new code will cause." Yardley continued:

> The new Ambassador will probably engage in the same sort of activities, but we may not be in a position to know just what is going on. Isn't it more desirable to keep this Ambassador here and know what he is up to than to have a new one without being certain that we can check up on his activities?

The State Department official responded:

> Yes we have thought of all that. My impression is the entire case will be dropped. It is too serious to meddle with.*

B. The KCIA Case: A More Recent Bribery Conspiracy

In the early summer of 1971, a U.S. intelligence agency reported to the Department of Justice the details of intensive KCIA lobbying of the House Foreign Affairs Committee and a substantial contribution to a U.S. Congressman. This information was communicated to C.D. Brennan, FBI Assistant Director in charge of the Intelligence Division, and to Assistant Attorney General Mardian in charge of the Department of Justice Internal Security Division. According to the Justice Department records, Mardian promptly contacted the FBI to determine whether the Bureau was investigating illegal transactions of government officials with the Korean government. He arranged for a personal review and an additional review by FBI officials of the intelligence reports "to determine if any action can be taken."

A few days later Bureau officials forwarded a summary of the reports, and the following conclusions and recommendations to Director Hoover:

> We have received no information regarding this matter from any other source and there is no data in Bureau files which would serve as a basis for the Bureau's conducting any active investigation. We are precluded from doing this based solely on (sensitive intelligence reports). Further, even if the allegations

---

* Yardley, Herbert, The American Black Chamber (1933).

> from these sources could be proven, it is doubtful that any prosecution could be sustained because of intended disclosures which would be required in court proceedings. The most logical action which might be taken would be in the hands of the Department of Justice, the Department of State or the White House and would be in the nature of administration action (sic) rather than prosecutive action.

Two days after this memorandum was written, FBI Director Hoover sent a similar memorandum to Attorney General Mitchell attaching a summary of the intelligence reports. Hoover's memorandum to the Attorney General reiterates the Bureau contention that it was precluded from instituting investigation based solely on such sensitive intelligence reports. Hoover affirmed the absence of independent material in Bureau files that could serve as the basis of any active investigation into the matter. Hoover also expressed his doubts to the Attorney General that any prosecution could be sustained because of attendant disclosures during court proceedings. Hoover then concluded:

> Information in the attached memorandum is also being made available to Dr. Kissinger at the White House. No further action is contemplated by this Bureau.

No further action was taken regarding the Korea affair until 1975.

C. The Khramkhruan Case: Narcotics Trafficking

The following narcotics trafficking case was discussed in great detail in hearings before a subcommittee of the House

Government Operations Committee in 1975.* During those hearings representatives of the Department of Justice and the CIA discussed the 1974 dismissal by the Department of Justice of an indictment against a CIA operative on national security grounds.

In 1973 a CIA operative from Thailand, Puttaporn Khramkhruan, was indicted for participating in the illegal importation of 25 kilos of raw opium into the United States. According to the testimony and a subsequent congressional committee report on the case, the CIA initially cooperated with Customs in investigating Khramkhruan's involvement in narcotics trafficking. Khramkhruan was indicted along with six other individuals in August of 1973. Originally he was to have been called as a government witness, and not to have been named as a defendant. However, Khramkhruan subsequently decided not to cooperate as a witness and announced that he intended to leave the country. Khramkhruan was arrested and served a superseding indictment naming him a defendant. At that point Khramkhruan announced that part of his defense would be that the CIA knew about his opium smuggling.

Initially the CIA had promised its cooperation, including provision of necessary documents and witnesses, to the Department of Justice. Indeed it even volunteered to provide a rebuttal witness to any claim by Khramkhruan that the CIA had

---

* Hearings before a Subcommittee of the House Government Operations Committee July 22, 23, 29, 31 and August 1, 1975.

advance knowledge of his narcotics trafficking.

However, shortly before the trial began the CIA notified the U.S. Attorney that it would not produce documents necessary for discovery under the Federal Rules of Criminal Procedures or pursuant to the ruling in Brady v. Maryland, 373 U.S. 83 (1963), nor would it provide a rebuttal witness on Khramkhruan's charge of CIA advance knowledge, nor would it comply with the so-called Jencks rule (18 U.S.C. 3500) requiring disclosure to the defendant of prior statements of government witnesses.

According to the testimony of CIA witnesses*, the CIA's request to the Justice Department for the dismissal of the indictment was based on the fact that prosecution would lead to discovery motions by the defendant which, when granted, would reveal sources and methods of ongoing CIA clandestine operations in Southeast Asia. The witnesses left unsaid the fact that CIA would find it embarassing to have one of its operatives found guilty of narcotics trafficking.

D. The Nha Trang Murder

The Army concedes the existence of a murder prosecution that was thwarted by national security considerations. However, the Army's records explain neither the facts leading to the prosecution nor how national security impinged upon investigation or prosecution. Because of the incompleteness of the record,

* Hearings before the Subcommittee on Government Information and Individual Rights of the Committee on Government Operations of the House of Representatives, July 28, 29, 30, 31 and August 1, 1975.

the Committee was forced to rely primarily on newspaper accounts and interviews.

In 1968 the Special Forces proposed to conduct an intelligence operation which would employ Vietnamese spies as trail-watchers operating on both sides of the Cambodian border. The written operational proposal had to be cleared by the CIA, the agency charged with coordinating intelligence responsibility and authority for U.S. forces in Vietnam. The proposal stated that any agent found to be working for enemy intelligence would be "terminated with extreme prejudice", a phrase allegedly interpreted by CIA to mean that the officer would be turned over to South Vietnamese legal authorities. CIA approved the operational proposal.

In the late spring of 1969, the Special Forces suspected that a spy it had employed in the operation was in fact a double agent who served North Vietnam intelligence. According to a CIA official interviewed by the Committee, the Special Forces consulted with the CIA and were advised in the methods of conducting a proper counterintelligence interrogation and investigation. According to this official, Special Forces personnel did interrogate the alleged double agent and, concluding that he was guilty, killed him, apparently mistakenly relying on the original operation proposal authority.

General Creighton Abrams learned of the incident and ordered a preliminary criminal investigation. A month later,

eight Special Forces officers were arrested in connection with the death. Defense counsel for the officers during discovery proceedings took testimony from a number of U.S. intelligence community employees. According to the CIA the transcripts of this testimony contained the details of a large portion of U.S. intelligence activities in Southeast Asia. Press accounts of the legal proceeding were extensive and public attention was focused on the upcoming trial.* A civilian lawyer for three of the Special Forces soldiers claimed that a representative of the Agency "hid behind executive privilege."* Based upon the discovery proceedings, this CIA officer assessed the likelihood of public disclosure of intelligence sources and methods during trial as very high.

On October 1, 1969, the New York Times reported that Secretary of the Army Stanley Resor announced that he had "decided to drop all of the charges in view of the fact that the Central Intelligence Agency would not permit members of its staff to testify."

In its recent memorandum to the Intelligence Committee, the Army Judge Advocate General's office stated,

> This office does not have a factual basis to verify the accuracy of the statement that, for reasons of national security, the Central Intelligence Agency would not make available any of its personnel as witnesses at the pending courts martial. On this basis, however, the charges were dismissed by the Secretary of the Army on 29 September 1969.

In further explanation, representatives of the Department of the

* New York Times, August 25, 1969.

Army stated that the Army can confirm that the case was dropped for national security reasons but all records of negotiations between the Army and CIA over witnesses and documents for use in the courts martial are no longer available at the Army.

In subsequent discussions with an official of the CIA, the Committee learned of a meeting between DCI Richard Helms, Attorney General Mitchell, and Secretary of Defense Laird. Those principals, with President Nixon's concurrence, decided that the case could not proceed for national security reasons and instructed Secretary Resor to drop the case.

E. The Watergate Case

The claim that intelligence activities must be protected does not need to be legitimate for it to interfere with investigations or prosecutions. Nor is it necessary that the intelligence community make the claim. A prime example of these two possibilities is the Watergate Case.

Within about a week of the Watergate break-in of June 1972, FBI investigators discovered evidence linking the burglars to an individual named Kenneth Dahlberg, and another individual named Manuel Ogarrio in Mexico City. This was a critical link that eventually traced the burglars to money in the Nixon reelection campaign and ultimately to the White House.

According to the House Judiciary Committee Special Impeachment Task Force report, as soon as the White House discovered that the Bureau had uncovered the connection, President Nixon directed Haldeman to meet with CIA Director Helms, Deputy Director Vernon Walters and John Ehrlichman to ascertain whether there was any CIA involvement in the Watergate affair. The Impeachment Task Force's report summarizes the results of that meeting as follows:

> The President directed Haldeman to ask Walters to meet with Gray to express these concerns and to coordinate with the FBI, so that the FBI's investigation would not be expanded into unrelated matters that would lead to disclosure of the early activities of the Watergate principals.

Although Helms had assured Haldeman and Ehrlichman that there was no CIA involvement in Watergate, he did direct his deputy to meet with the FBI Director and to remind the FBI of the agencies' agreement that if either agency appeared to be running into each other's sensitive operations, that they were to notify each other and back away.

In a memorandum from Helms to Deputy Director Walters dated 28 June 1972, Helms gave the following directions:

> In short at such a meeting (between Walters and Gray), it is up to the FBI to lay some cards on the table. Otherwise we are unable to be of help. In addition we still adhere to the request that they confine themselves to personalities already arrested or already under suspicion, that they desist from expanding this investigation into other areas which may well eventually run afoul of our operations.

According to Walters' testimony before the Senate Watergate Committee, Helms again reminded Gray of this arrangement on their way out of the White House after their meeting with Haldeman and Ehrlichman.

In a memorandum for the record dated June 28, Walters summarized his meeting with Acting Director Gray as follows:

> I recall that the FBI and the Agency had an agreement in this respect and that the Bureau had always scrupulously respected this. Gray said he was aware of this and understood what I was conveying to him.

For about a week the FBI did not proceed with the investigation because it was under the impression that it had indeed stumbled across a CIA operation and for national security

reasons felt that further investigations would jeopardize sensitive information and operations. In fact no such operation was involved but it is possible that Helms and Walters were not sure at that time whether a CIA operation was involved. The Watergate case, therefore, illustrates how such arrangements could be used, especially by White House officials, to obstruct a legitimate investigation.

VI. PAST LEGISLATIVE AND ADMINISTRATIVE PROPOSALS IN RESPONSE TO THE "GRAY MAIL" PHENOMENON

Over the years the CIA and its predecessors have responded with two initiatives to the problems of enforcement of the espionage and other statutes which risk disclosures of foreign intelligence "sources and methods". First, especially with respect to leaks and espionage violations, military and civilian intelligence agencies have called for enactment of statutes similar to the British Official Secrets Act. Second, since 1954 the CIA has sought special arrangements with the Department of Justice designed to avoid controversies in these kinds of cases by relieving CIA of its responsibility to report to the Department criminal activity where further investigation might, in CIA's judgment, jeopardize clandestine operations.

A. Legislative Initiatives: Abortive Efforts to Enact An Official Secrets Act

Obviously, some of the problems described earlier in the administration of espionage statutes would be resolved if the culpability requirements were eased. It would be immensely easier to prosecute leaks and espionage if all that had to be proven was that the defendant had passed classified information to unauthorized persons -- essentially the rule under the Official Secrets Act.*

According to Professor Benno Schmitt of Columbia Law School, one of the nation's experts on our espionage statutes, proponents

---

* It should be noted that the Official Secrets Act not only applies to divulgence but also to publication of secrets, and that its scope extends to all official government information, not just national security secrets.

of such legislation "reached back to Civil War experience, in which the Union cause had been hindered by newspaper detailing of military plans prior to their execution." The most famous confrontation in the Congress over this kind of legislation was during the Wilson administration when, according to Professor Schmitt, the administration "proposed to censor or make punishable after the fact (exactly which option was never made clear), publication of defense information in violation of Presidential regulations, without any limiting culpability requirement." According to Schmitt:

> In response to this proposal, the Congress engaged in its most extensive debate over freedom of speech in the press since the Alien and Sedition Acts. The preoccupation was not an academic one. Opponents feared that President Wilson or his subordinates would impede, or even suppress, informed criticism of his administration's war effort and foreign policy under the guise of protecting military secrets...The aggrandizing of presidential powers during wartime was a recurrent fear of Republicans, especially Senate progressives such as Borah, LaFollette, Norris and Hiram Johnson.

The proposal was ultimately voted down and only the more modest of the Wilson administration's espionage proposals were adopted. That legislation serves as the framework for our present espionage statutes.

Similar proposals were made during the World War II period. In 1946 the Joint Congressional Committee for Investigation of the attack on Pearl Harbor recommended that Congress enact legislation prohibiting the revelation of any classified information. During the war there had also been a study jointly conducted by Army and Navy Intelligence and the FBI which made

similar recommendations transmitted by the Secretary of War to the Attorney General in June, 1946.

In 1947, the predecessor of Section 798, making it a crime per se to reveal communications intelligence, was introduced and in September of 1948 an omnibus bill was proposed by the Truman administration incorporating the Section 798 language and a number of earlier proposals for simplifying the culpability requirements of the espionage statutes. During this period the CIA, objecting to what it called a "piecemeal" approach of amending various sections of the espionage statutes to deal with special limited problems, suggested a redrafting of the whole espionage statute along the lines of the British Official Secrets Act. A few of the technical changes proposed by the Truman administration, and the intelligence and the military departments were incorporated into Title 18; the most significant of those was Section 798 of Title 18. However the intelligence community and Department of Defense were not satisfied with those amendments and in 1952 Defense Secretary Robert Lovett proposed to President Truman that the administration still seek legislation similar to the British Official Secrets Act. The Justice Department prepared such legislation but it did not reach the floor in either House.

In 1957 the Commission on Governmental Security suggested legislation that would make it a crime "for any person willfully to disclose without proper authorization for any purpose whatsoever, information classified, knowing such information to have been so classified." The Commission justified its proposal in terms of the "gray mail" problem":

> Since espionage cases may frequently involve national security information of the highest classification, the government is confronted with a serious problem of how far such information can be compromised in the course of prosecution...A defendant who may have met with the greatest success in securing our most precious secrets, may also have secured an advantage in warding off successful prosecution.

No action was taken on the Commission's recommendation, nor on subsequent initiatives in 1958 in the Eisenhower administration, nor a similar initiative in 1966 by the CIA. Indeed, legislation was never seriously considered in this area until the Federal Criminal Code Reform legislation was introduced by the Nixon administration. That legislation contained some of the recommendations suggested by the intelligence community in the past but met with strenuous opposition from media and civil liberties groups. Similarly, those same groups strongly criticized legislation drafted by the CIA and proposed by the Ford administration in February of 1976. No action has been taken on the CIA proposal.

Typical of opposition that the Federal Criminal Code Reform and the subsequent Ford administration proposal provoked is the testimony of Jack Landau of the Reporters Committee for Freedom of the Press before a Congressional subcommittee which was considering the Federal Criminal Code Reform:

> It is abundantly clear that S. 1 (the Code reform proposal) is an unwise and unconstitutional proposal which could be used to silence the type of aggressive news reporting which produced articles about the Pentagon Papers, the Mylai massacre, the Watergate cover-up, the CIA domestic spying, the FBI domestic spying and other government misdeeds. News reporting which has been embarrassing to some persons in the government and which is dependent in whole or in part on government compiled information and reports frequently supplied to the press by present or former

government employees without government authorization.

The new espionage provisions of the Federal Criminal Code Reform were dropped prior to its consideration by the Senate early this year; proponents realized that any further action on the Federal Criminal Code Reform would be indefinitely postponed as long as there was significant controversy over its constitutionality.

B. Administrative Initiatives

In February of 1954 Lawrence Houston, General Counsel for the CIA, established an arrangement with William Rogers, Deputy Attorney General, to obviate the need to report to the Department of Justice certain criminal activity coming to CIA's attention. According to a memorandum by Houston to Allen Dulles, Houston justified this arrangement to Rogers in the following terms:

> Occasionally, however, the apparent criminal activities are involved in highly classified and complex covert operations. Under these circumstances, investigation by an outside agency would not hope for success without revealing to that agency the full scope of the covert operation involved as well as this agency's authorities and manner of handling the operation.

Apparently, Rogers agreed with this assessment and "saw no purpose in referring the matter to the Department of Justice" under the circumstances. There is some uncertainty in the materials the Committee has reviewed as to whether this arrangement was ever to have been reduced to writing or any formal understanding between CIA and the Department of Justice.

The ambiguity of the arrangement is highlighted by an exchange of correspondence between the CIA and the Bureau of the Budget in

August of 1954. The CIA expressed concern regarding legislation about to be enacted which would grant the Attorney General exclusive responsibility for investigating all violations of Title 18 by government officers and employees. Notwithstanding the CIA's concerns, that legislation was eventually enacted and codified as 5 U.S.C. Sec. 311(a) (since recodified in 28 U.S.C. Sec. 535(b)(2), see Appendix).

In November of 1958, Rogers sent a memorandum to the heads of all departments and agencies in the Executive branch of government emphasizing their responsibilities under the legislation. Subsequent Attorneys General have issued the same reminder soon after taking office. However, for over twenty years the CIA, based on its 1954 arrangement, assumed these directives exempted reporting the kinds of cases Houston had described to Rogers. Although there were minor changes in the procedures described in Houston's original memorandum -- in 1955 and again in 1964 -- the basic thrust of the arrangement wherein CIA took primary responsibility for balancing the need for secrecy against the administration of justice remained until 1975.

In January of 1975 DCI William Colby and Lawrence Silberman Acting Attorney General, reviewed the 1954 arrangement. At that time Silberman took the position that the agency should comply with 5 U.S.C. Sec. 311(a) by providing a summary "but not an investigative report as such" in essentially every case and that the basic security issue should be raised, but that the Attorney General, not the CIA, would make the decision on whether or not to prosecute.

The responsibility of the CIA to report evidence of crimes by its employees to the Attorney General was the subject of a specific provision in Executive Order 11905 issued by President Ford (designed to regulate the activities of the intelligence community) and its successor issued by President Carter, Executive Order 12036.

The Attorney General and DCI have recently signed a memorandum of understanding which would serve as a successor to the 1954 arrangement.* The new Executive Order and the new memorandum of understanding between Justice and CIA retain the principle established by acting Attorney General Silberman that the Department of Justice has the responsibility of balancing the needs of secrecy against the ends of justice.

Both the memorandum of understanding and the Executive Order purport to impose a burden on the intelligence community to report criminal acts by its own employees. With respect to non-employees, the new Executive Order reads as follows:

> ...(the head of any intelligence agency must) report to the Attorney General evidence of possible violations by any other person of those federal criminal laws specified in guidelines adopted by the Attorney General.

No such guidelines have yet been adopted and, therefore, the reporting requirements under that provision are unclear. Furthermore, neither the memorandum of understanding nor the Executive Order addresses the way in which the Department of Justice should handle evidence necessary to investigate or prosecute an allegation brought to its attention under these provisions. In other words, neither the memorandum of understanding nor the Executive

---

* The Committee has been informed that this memorandum may be subject to further revision.

Order is intended to resolve the controversies on the use of classified information in the prosecution, the problem to which this report is addressed.

Certainly one of the difficulties in developing these policies is concern that these reporting requirements might indirectly involve the foreign intelligence agencies in domestic law enforcement in violation of the 1947 National Security Act. The Committee shares this concern. However, the solution to this dilemma may be in the distinction between passively reporting domestic criminal activity on the one hand and actively seeking it out (e.g., "watchlisting" domestic subversives). The drafters of future versions of the memorandum of understanding and guidelines implementing the Executive Order should keep this distinction in mind and avoid an unrealistic interpretation of the domestic law enforcement prohibition.

VII. NEW INITIATIVES

The Committee agrees with former DCI Colby's testimony before the Subcommittee on Secrecy and Disclosure that, "We would be irresponsible if our revision of intelligence structure did not recognize the need to protect the necessary secrets of intelligence better than we do today." A resolution of the dilemma presented by this report must be a part of the charter legislation being considered by the Intelligence Committee.

To meet the problems set out in this report, the Committee has prepared a recommended program.* This program is designed to serve two basic ends: first, to facilitate the enforcement of espionage statutes and thereby protect our national secrets without jeopardizing constitutional principles; and second, to facilitate enforcement of the criminal sanctions set out in the legislative charters. Without question, the movement to apply the rule of law to intelligence through statutory charters will be severely undermined if leakers or spies continue to go unpunished or if violations of the charters go unenforced.

Although unanimity exists among the members of the Committee on the scope and significance of the problem of "gray mail", there is substantial disagreement on a remedial program. Some members such as Senator Wallop (see separate views) describe the recommendation of the Committee as resulting in only marginal improvements. Other members find his approach or any major recasting of the espionage laws to be fraught with the practical, legal and political problems which have thwarted efforts to remedy this problem in the past. This is not to say that the espionage statutes written over six decades ago should not be subject to a serious re-examination. There is strong sentiment that the committee should undertake such a study but the implementation of the program recommended herein should not await the completion of that study.

The program the committee does adopt, is, however supported by those who would take an even more fundamental approach, as being the minimum dictated by the record disclosed in this report. In

---

* See pp. 62 ff.

the end the committee recognizes that if this program were adopted in toto there would still be circumstances where some leaks would go unpunished and some prosecutions subject to "gray-mail" but perhaps that is the price we must pay for the constitutional protections of a free press and a right to a public trial.

A. Leaks, Espionage, and Current Law

The espionage statutes clearly cover most forms of traditional spying. Nevertheless, prosecutions under these statutes have often failed in the face of the "gray mail" phenomenon.

Leaks differ qualitatively from espionage. A leaker normally discloses classified information not to a foreign agent but to a journalist. In fact, this type of security leak has become part of a flourishing informal and quasi-legal system. For example, senior officials often disclose classified information as a means of explaining their positions to the public, while dissenters leak in order to expose improprieties and shoddy thinking.

There are two major drawbacks to the sub rosa practice of providing selected intelligence information to the news media and other sources. First, the public does not necessarily receive a balanced view from the leaked information because the process is informal. Second, and more importantly, information whose secrecy is vital to our national security is sometimes disclosed.

Under current law, it is not at all clear whether most leaks of information to the media are criminal. To the legal neophyte in this field, it appears that Title 18, §793(d) and (e) do address

the problem. §793(d) and (e), in similar language, make criminal the behavior of any person who, having lawful or unauthorized,

> access to . . . information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States . . . willfully communicates . . . the same to any person not entitled to receive it.

Superficially then, this statute seems to punish leaks to journalists as well as spying. However, these statutes are not normally used in cases unless transmittal of information to foreign agents is involved. Whether they could be used in cases where information is passed to a journalist is unclear from a careful reading of the legislative record. This very lack of clarity and Congressional reticence to clarify the statutes, discussed earlier, has in fact discouraged leak prosecution under these sections which in turn has precluded the growth of case law to define the statute's meaning. Application of the statute to publication of national defense information by a newspaper raises serious First Amendment problems. Two distinguished commentators have suggested that after taking into account constitutional concerns, there is "little worth preserving in these two remarkably confusing provisions."* As noted earlier, this Committee has no desire to decide in this report whether these statutes perform a necessary task or whether they do it adequately. However, it does believe the administration should itself decide under what, if any, circumstances it will seek to apply

---

* Harold Edgar, Benno Schmitt. "The Espionage Statutes and Publication of Defense Information," 73 Columbia Law Review 930.

criminal sanctions to leaks of national security information.

Administrations from the time of World War I have put forward proposals that would resolve the ambiguities of the law regarding leaks by making the disclosure of government secrets a crime even without requiring proof of damage to the national security. In fact, practically all of these attempts have floundered in part because Congress has refused to make leaks explicitly criminal which do not damage the national security.

Although the mere classification of a document may not in itself warrant criminal penalties for its disclosure, certain narrow classes of information are in fact so sensitive that a statute should protect them against any disclosure. Thus, communications intelligence is protected against disclosure even without proof of harm or communication to a foreign agent.

Former Director Colby testified in favor of a proposal that would impose such strict liability penalities upon the unauthorized disclosure by government employees of sensitive sources and techniques of intelligence collection. To an extent the Committee anticipated Colby's recommendation in a provision of its proposed legislative charter (S. 2525, Sec. 431(a)). This section penalizes the disclosure of the identity of a CIA employee serving under cover in a manner which jeopardizes the safety of that employee. The Committee believes that such a statute

would cover the type of unauthorized disclosure recently made by former CIA employee Philip Agee. Colby, however, suggests that the sanction be expanded to cover CIA sources as well as employees and circumstances where political or economic reprisals could be expected. Although Colby urges protection for intelligence "techniques," the Committee is extremely hesitant in going beyond the strict liability coverage already accorded communications intelligence. Colby himself warned the Committee of the great difficulties inherent in developing a workable definition of "technique." Added to the difficulty of legally defining

"technique" are the difficulties of proving that any given disclosure revealed it.

As this report clearly establishes, great difficulties exist in enforcing current espionage statutes due to the "gray mail" phenomenon and any new statutes would face the same problem. Even under the "strict liability" of Section 798, the law is unclear as to whether the prosecution would have to establish that the classification of the material is substantively valid. If so, the government would face the prospect that much sensitive information would have to be revealed in the course of litigating that question.

The modest expansion of the espionage statutes to cover disclosure of agents under cover warrants serious consideration, despite the risk of "gray mail." However, the Committee is not prepared to recommend a major restructuring of those statutes to encompass all leaks. First, in light of the experience under Section 798 of Title 18, most members of the Committee have serious doubts as to whether even a radical restructuring of the rest of the espionage law along the lines of the British Official Secrets Act could have an appreciable impact on leaks. Second, the Committee is unanimous in the view that countless practical, legal and political differences lie in the path of such an undertaking.

What other than criminal sanctions will diminish the frequency and gravity of leaks? Any comprehensive law

against leaks cannot be effective so long as it is impossible to distinguish between a criminal act and a widely accepted governmental practice. Past Executive Orders on classification have failed to protect the most important national security information by providing for the classification of much information that ought to be made public. Recently, President Carter promulgated a new order dealing with secrecy and classification. This new Order is an improvement over past practices, but if it is not strictly construed and vigorously enforced, it will foster disrespect for the whole classification system. In the words of Justice Stewart in the Pentagon Papers case: "When everything is secret, nothing is secret." Perhaps the mechanisms contained in the new executive order will avoid overbroad classification and will allow for declassifying intelligence necessary to informed public debate and thus minimize the incentive behind unauthorized disclosure of information.*

Yet, given the ingrained nature of the leaks system and the fact that leaks often result from bureaucratic infighting, some unauthorized disclosure is bound to continue. To deal with leaks administrative sanctions are better suited in most cases than criminal ones because they are more enforceable.

---

* Of course, such a declassification system must be impartial. Otherwise, the public will be faced with a biased view and officials disagreeing with this view would have added incentive to leak.

No risk of "gray mail" would exist, because proceedings could be secret. Due process rights--these might include a right to present evidence, to be represented by counsel, to challenge accusations, and to appeal to the courts--must, of course, be preserved. At the same time, administrative sanctions would be less onerous. Dismissal or loss of security clearance are at times more appropriate sanctions for leaking than criminal prosecutions.

B. Facilitating Enforcement of Existing Statutes and the Charters

The review of the cases described earlier and the hearings of the Secrecy and Disclosure Subcommittee have led the Committee to recommend a program of both administrative and legislative action designed to facilitate enforcement of the espionage statutes. In essence, on the administrative side, the Committee recommends a streamlining of decision-making within the Executive branch on cases where leaks or espionage occur and the use of administrative sanctions in less serious breaches of security or other violations of the law. On the legislative side, the Committee recommends some new judicial procedures intended to strengthen the hand of the judge and encourage accommodation between the defendant and the prosecutor concerning the use of classified information in litigation -- to seek solutions which encourage proceeding with prosecution rather than dropping the case out of fear of disclosure of sensitive information.

(1) Administrative Recommendations

At the heart of its administrative recommendations (see pages 62-64) is the Committee's concern that there is no effective administrative system currently operating in the Executive branch for investigating and penalizing unauthorized disclosures and the crimes of bribery, perjury and others described in Part V. Leakers occasionally are penalized on an ad hoc basis.* Violations of the Executive Order on classification, and even espionage, are not subject to formal administrative sanction.

In the case of leak investigations the FBI takes the position that it should not investigate a leak unless there is clear evidence of a crime. The Committee also believes that the FBI should not conduct investigations of citizens for leaks without their consent except in cases involving a nexus with criminal activity.

But where there is such a nexus, even where prosecution of the crime is impossible because of the risk of further disclosures, the FBI should investigate when the leak endangers sensitive intelligence sources or methods and is reasonably believed to violate the criminal statutes of the United States.

---

* E.g., Donald Stewart, formerly the chief leak investigator for the Department of Defense, supplied examples of cases during his tenure when high-ranking military officials received a "slap on the wrist" for what appeared to be serious compromises. Mr. Stewart's prepared statement appears as part of the Subcommittee's public hearing record.

The persons investigated should be officials, employees, or contractors of the executive, legislative, or judicial branch having access to the information leaked; the investigation and any intrusive investigative techniques should be authorized in writing by the Attorney General;* and the investigation should terminate within 90 days, unless such authorization is renewed. The Attorney General should submit information concerning the leak to the head of the employing agency, or to the President, for appropriate administrative action.

These standards do not go as far as the recommendations of the Rockefeller Commission (on alleged CIA abuses), which proposed FBI investigations without evidence of a crime or the Attorney General's approval. Nevertheless, they break sharply with current Justice Department policy foreclosing FBI investigations of damaging criminal leaks where administrative action, rather than prosecution, is the intended result.

The Justice Department is properly concerned that such cases waste time and money because they often turn out to be leaks either formally or informally sanctioned by appropriate authorities. Nevertheless, where such a leak endangers sensitive sources or methods and violates the criminal statutes investigation is appropriate.

The Director of Central Intelligence has extraordinary powers under the 1947 National Security Act, and he and the

---

* Court orders would be required for electronic surveillance or searches and seizures; such techniques would rarely be appropriate in most "leak" cases.

director of the National Security Agency would have similar authority under the proposed legislative charters, to dismiss their employees. These charters should also recognize the authority of the directors of CIA and NSA as well as that of the heads of other agencies to take disciplinary action against employees who leak classified information. With that authority should come the implied responsibility of the agencies to investigate employees' past activities which would warrant action.

The leak cases reviewed indicate that these initial investigations are often not conducted because no one official at the intelligence community level has the authority to require individual agencies to pursue particular leads in an investigation. Some intelligence community body should be required to ensure that individual agencies investigate activity by intelligence agents, employees or informants which violates security or charter prohibitions. However, this investigative responsibility should not be delegated to the FBI until there is evidence of criminal violations.

As stated, the advantage of administrative sanctions over criminal prosecution is that procedures under the former do not require extensive public disclosure of classified information. Therefore, both the staff of the Committee and representatives of the Executive branch should explore what possibilities exist for formalizing and upgrading

administrative review and investigation procedures for violations of security and other unlawful acts by intelligence officials. For example, a possible alternative is an administrative review procedure for employees similar to courts martial in the military. Officials of the agency would hear complaints of violations, especially in circumstances where the decision has been made to forego criminal proceedings for national security reasons. These administrative review procedures could be applied to former employees who violate charter prohibitions, assuming that a deferred compensation pension plan could be conditioned upon continued compliance with security and charter requirements. Former employees who violate prohibitions could be made subject to loss of pension rights through the administrative procedure, if it were made clear in the pension agreement that payments were contingent on such compliance. A decision to take away pension rights would presumably be reviewed by the courts to ensure that no former employee's rights were violated.

Another major goal of the Committee recommendations for administrative action is to improve accountability in Executive branch decisionmaking concerning cases involving national secrets. The Committee agrees with the testimony of Philip Lacovara before the Secrecy and Disclosure Subcommittee:

> I have the sense that the government may be aborting cases prematurely or unnecessarily because

> of a failure to press the alternatives to their fullest, as we did, for example, in the Special Prosecutor's Office in the Ellsberg break-in prosecution, where defense efforts to use "national security threats" to stymie the case were beaten in the courts.

During the course of the hearings the Subcommittee members and witnesses agreed on a number of fundamental points about decisionmaking in these cases. There is little controversy that the ultimate decision on whether to proceed on these types of cases must be centralized within the Attorney General's office. Nevertheless, the DCI should have authority, through the "sources and methods" provision of the National Security Act, to make his views known on whether to halt prosecution of a criminal case. The Deputy Attorney General and the DCI in testimony before the Subcommittee agreed that it was up to the Attorney General, with disputes settled by the President, to decide whether or not the jeopardy to national secrets in pursuit of a prosecution outweighs the ends of justice.

If the intelligence community disagrees with an Attorney General's decision, the DCI or any other agency head should have the right to appeal to the President. The decision to drop a national security case should be made in writing by a high-level official within the Department of Justice, an Assistant Attorney General or a Deputy Assistant Attorney General. Included in that written decision should be a

detailed explanation of the information which would have been revealed in the course of trial, why the information would be revealed, and what damage the disclosure of the information would have to the national security. The mere fact that a written record must be made will discourage thoughtlessly dropping a potential prosecution.

A final area appropriate for administrative action pertains to the requirement that intelligence agencies report to the Department of Justice evidence of criminal activity by employees. As noted in Part VI of this report, the administration is currently at work attempting to implement provisions of the new Executive Order and has recently updated the so-called Silberman-Colby understanding as to the requirements of the intelligence community to report crimes of its employees to the Department of Justice.

If there is no mechanism through which the Department of Justice is so notified, the law enforcement process is likely to break down. The guidelines should be promptly issued and the Attorney General and the DCI should quickly determine whether any further revisions are necessary in the memorandum of understanding on reporting crimes by employees. It is equally important that either the prospective guidelines or an expanded memorandum of understanding address not only criminal activities of intelligence agents, employees or assets, but also criminal activity known by the intelligence community which does not involve its employees or assets.

Such an understanding must consider the protection of sources or methods.

(2) Legislative Initiatives

The purpose of the legislative suggestions set out in Part VIII is to provide alternatives which will allow prosecutors to avoid what one witness described as the "disclose or dismiss dilemma." Because of ambiguities in existing judicial procedures or because of a general reluctance on the part of the intelligence community and the Department of Justice to take the chance of pursuing these cases, the administration must decide whether to disclose intelligence information or to dismiss a criminal case or not pursue an investigation at the outset.

However, the dilemma posed by the introduction of sensitive intelligence information into criminal cases, especially at the behest of the defendant, can frequently be avoided because the information is requested for an irrelevant matter. For example, Lacovara described to the Subcommittee the following sequence in the prosecution of the Watergate burglars for the break-in of Dr. Ellsberg's phychiatrist:

> After the indictment was returned, the defendants did in fact demand the production of highly classified files, including nuclear missile targeting plans. The defendants were seeking to utilize discovery to obtain national security information in order to support the purported defense that they believed the break-in was justified by national security concerns. The special prosecutor argued, however, and both District Judge Gesell and the U.S. Court of Appeals for the District

> of Columbia Circuit agreed, that the information sought was irrelevant because "good faith" motivation was not a valid defense against the crime charged, conspiracy to violate Fourth Amendment rights. Thus the difficulty of choosing between forfeiting an important criminal prosecution or disclosing information potentially damaging to our national security was avoided.

In many other cases it is possible that if the prosecutor had forced the court to carefully examine the relevancy of the intelligence information to a purported defense or motion, the judge may well have been forced even under the present standards of relevancy to decline the request for the information. However, administration witnesses were reluctant to rely on the relevancy standard. They argued that what one judge found relevant another judge would find irrelevant and that many judges grant the discovery motion first before deciding whether or not the intelligence information will be used in the case. Furthermore, defense counsel routinely make sequential discovery motions which harrass the prosecution and thus tie up the prosecutors in negotiations with the CIA over sensitive documents.

Mr. Lacovara suggests that Congress enact an omnibus pretrial proceeding for use in all cases where classified exhibits or testimony would be required. The defendant would be required to put the prosecutor and the court on notice in advance of trial of all motions he would make requiring discovery of sensitive classified intelligence information when he might have reasonably known of the need for discovery

prior to trial.* He would have to argue successfully the relevancy of each motion before the court in order to secure discovery of the documents or testimony. For the purposes of argument, the court could assume that the documents existed without actually providing the defendant the documents and could decide in advance whether the defense would be permitted or the motion granted as a matter of law. This process would be intended to "weed out" irrelevant defenses and thus simplify prosecution of the case. If at some later time a new matter arose requiring a special motion or defense which in turn required the disclosure of secrets, the court could still entertain an appropriate discovery motion and both the government and the defendant would be entitled to an interlocutory appeal.

If such a special omnibus procedure is adopted, the Committee recognizes that there will be cases where the "weeding out" process will actually arrive at motions and defense arguments that are relevant and do require the use of intelligence information. At that point the judge must decide two basic questions: (1) Is the information in question truly national security information, the disclosure of which would damage the national security? (2) What action should he

---

* Of course, if the prosecution is to go forward, the government must turn over all materials relevant to the defense notwithstanding the fact that some of them may be classified. See, supra, p. 21.

take against the prosecution if it withholds the documents or testimony (e.g., dismissal of the case)? Of course, the Government always has the option of dismissing a prosecution if the court's decision on these matters would require what it believes to be excessive disclosure.*

In 1974 the Supreme Court proposed the Federal Rules of Evidence. These Rules of Evidence were extremely controversial in the Congress because they contained a provision, Section 509, that defined a "secret of state" privilege. An invocation of the privilege by the government would prompt an in camera adversary proceeding in which the parties would litigate whether the information in question was in fact "a secret of state."

Section 509 was rejected by the Congress as it reviewed the rules proposed by the Supreme Court. However, several witnesses agreed that perhaps Section 509 might serve as the basis for an in camera adversary proceeding that would resolve the use of intelligence information in the course of a trial after the "weeding out" process described above. Furthermore, several adjustments to the Section might be made to respond to criticism which led to congressional rejection in 1974. For example, the new state secret privilege might more narrowly define the types of information to which the government could invoke the privilege. It might give a greater role to the

---

* The Government does not undertake prosecution on a whim. In deciding to drop an indictment the Attorney General must weigh the expenditures of time and money in investigation and prosecution, as well as fairness to the defendant who must live with the stigma of an unchallengeable indictment.

court in reviewing the claim of privilege, including authority to go beyond and behind the classification to determine the actual damage to the national security if the information were disclosed. It might guarantee the presence of the defendant and his counsel in the in camera procedure, subjecting both to contempt of court and possible espionage prosecution if they disclose the results of the procedure.

The primary purpose of such a procedure would be to set standards to place the prosecution and the government on notice in advance on what types of information could be subject to privilege and to give the judge primary responsibility for administering the privilege. Lacovara in his testimony emphasized the importance of providing judges with some guidance as to what action should be taken if they find the privilege is legitimately invoked. Lacovara suggests a "sliding scale" of sanctions available to the judge so that "the remedy available to the defendant would vary depending upon the circumstances of the case." Lacovara goes on to further describe his proposal as follows:

> At one end of the scale, for example, if the defendant's possible use of the information is totally speculative, the case simply would continue without disclosure. At the other end of the scale, where the information is central to the question of guilt or innocence and where no other alternative to public disclosure is possible, dismissal may be necessary. In between, procedures such as instructing the jury to assume that the missing information would have proven a given proposition may be possible. Certainly the Department of Justice should press for some intermediate treatment like that before deciding that the case must be abandoned.

VIII. RECOMMENDATIONS

The recommendations which follow were formulated by the Secrecy and Disclosure Subcommittee and are endorsed by the full Committee. They will serve as an agenda for the Committee as it proceeds with consideration of legislative charters. The Committee will be developing specific legislative proposals to implement these recommendations for inclusion in the charters to be discussed in the course of its ongoing hearings. It is the Committee's hope that the Executive branch will work with the Committee on these matters and, in particular, on its recommendations for administrative action.

I. At this time Congress should focus primarily upon developing statutory and administrative procedures which would facilitate enforcement of the espionage law and other statutes subject to the "gray mail" phenomenon. The Committee is not prepared at this time to recommend a general recasting of the federal espionage statutes along the lines of the British Official Secrets Act. However, limited further protection of intelligence sources, especially the identities of agents and employees under cover, appears to be necessary.

II. The Executive branch should interpret the new Executive Order on security classification with an emphasis on decreasing the amount of unnecessary secrecy. The intelligence community, the Intelligence Oversight Board, and the intelligence committees of the Congress should declassify as many as possible of their reports and studies on matters of public concern to discourage the "leaking" of versions which have not been sanitized to protect "sources and methods" information. These reports and studies must be declassified in a disinterested manner, so that the public receives the true view of a given situation.

III. Administrative procedures for disciplining employees responsible for violations of security or other laws

should be developed. At the same time the intelligence community should centralize responsibility, perhaps in the Intelligence Oversight Board, for investigations of breaches of security and all violations which do not constitute crimes. The purpose of these procedures would be to permit sanctions against employees through internal agency procedures in which it is easier to cope with classified documents or testimony than in traditional public criminal trials. In many leak cases administrative sanctions may be more appropriate than a criminal conviction. Of course, these administrative proceedings would grant due process rights to the employee. Some consideration should also be given to applying these administrative review procedures to former employees through withdrawal of pension rights for former employees who violate security.*

IV. The FBI should continue to have exclusive responsibility for investigating criminal violations involving the intelligence community. In leak cases the FBI should initiate investigation when:

(1) the leak endangers sensitive intelligence sources or methods and is reasonably believed to violate the criminal statutes of the United States;

(2) the persons investigated are officials, employees, or contractors having access to the information leaked;

(3) the investigation and any intrusive investigative techniques are authorized in writing by the Attorney General;**

(4) the investigation terminates within 90 days, unless such authoriztion is renewed; and

(5) the Attorney General submits information concerning the leak to the head of the employing agency, or to the President, for appropriate administrative action.

V. The Attorney General should issue guidelines under the authority of Executive Order 12036 on the responsibility of the intelligence community to report crimes to the Department of Justice. The guidelines should cover reporting of all activity in violation of U.S. laws coming to the attention of the intelligence community, but must consider protection of sensitive sources and methods.

---

* For discussion of the Committee's rationale for recommendations III, IV, V and VI, see pp. 51-57, supra.

** Court orders would be required for electronic surveillance or searches and seizures. Such techniques would be considered appropriate in most "leak" cases.

VI. The Attorney General should issue regulations that are binding upon all departments of the government which set out the procedures whereby agencies of the intelligence community are to provide necessary information to attorneys of the Department of Justice to proceed with a criminal investigation or prosecution. The regulations should also set out how the decision is to be made not to proceed in national security cases and who is authorized to make such a decision. These regulations should require that any such decision be made in writing, and the decision paper should include the precise intelligence information which would have been disclosed in the course of the trial, why the official believes it would have been disclosed, and the damage the information would have to the national security if the case proceeds. The decision paper should be available to the intelligence oversight committees of the Congress and such cases should be reported to the committee annually or as required.

VII. Congress should consider the enactment of a special omnibus pre-trial proceeding to be used in cases where national secrets are likely to arise in the course of a criminal prosecution. The omnibus procedure would require the defendant to put the prosecution and the court on notice of all motions or defenses or arguments he intended to make which would require the discovery and disclosure of intelligence information or the use of intelligence community witnesses. The judge would be required to rule in advance of the trial on the admissibility of the intelligence information and on the scope of witnesses' testimony as well as the general relevancy of the motion or defense prior to granting discovery of any intelligence information to the defendant. On the other hand, the defendant would be permitted a discovery motion during the course of trial if the prosecution presents a matter not originally suggested by indictment or for which the defendant could not fairly have been expected to be on notice at the time of the omnibus procedure.*

* For a discussion of the Committee's rationale for recommendations VII and VIII, see pp. 57-61, supra.

VIII. The Congress should reconsider the secret of state privilege proposed by the Supreme Court in 1974. That privilege needs to be considerably revised along the lines described above but at a minimum should provide for an in camera adversary procedure on the privilege, define the scope of the privilege, the standards for its invocation, provide increased judicial authority for its procedural administration, and provide a sliding scale of sanctions available to the judge in the case where the privilege is successfully invoked.

Additional Views of Adlai E. Stevenson
October 6, 1978

The Report on Secrecy is a positive step, as far as it goes, but in my view it unnecessarily stops short of tackling the need for new laws to cover espionage and other unauthorized disclosures.

The Report emphasizes improvement of procedures to enforce existing laws -- which could aid enforcement of new laws as well. However, I believe the Senate Select Committee on Intelligence should recommend criminal laws that will address the threat to national security from breaches of security.

The laws affecting espionage are sparse. Those which treat leaks are almost non-existent. Grave damage can be done to the national security through purposeful leaks which may violate no statute.

New laws should not relate only to information derived from intelligence sources and methods; sensitive information derives from many sources. A State Department or White House official could improperly release information just as damaging as information which happens to be labeled "intelligence." The law should be drawn accordingly.

The Report's brief mention of the court martial system deserves fuller consideration to see if it could legally serve as a model for civilian officers who handle government secrets. The uniform code of military justice provides a

67

system whereby errant members can be disciplined without breaching their constitutional rights. Any such arrangements could, of course, provide for appeal procedures and congressional oversight. It might also be possible to require officers entrusted with government secrets to enter contractual arrangements by which they would agree to submit to special disciplinary procedures should they violate their contractual and legal obligations.

I urge the Committee to address the inadequacy of existing laws. It is not enough to support the improved enforcement of laws which do not exist.

THE SEPARATE VIEWS OF SENATOR MALCOLM WALLOP

The Committee's report amply documents the quandary variously known as "disclose or dismiss" or as "Grey Mail." Because prosecution requires disclosure of information likely to compound damage to the nation, leakers and spies have been allowed to go unpunished. The sensitive substance of the documents stolen or leaked must be discussed in open court because the court cannot assume that the documents were properly classified in the first place. Therefore, the courts have refused to enforce Sec. 793, Title 18 U.S.C., intended to punish anyone for revealing classified information, without first determining what the proper classification of the information should have been. Courts cannot avoid this function, because the classifying authorities cannot be deemed infallible or disinterested. Only an impartial determination of the proper classification can form the basis for judicial punishment of leakers and spies.

The Committee's analysis of the possible ways out of the quandary is circumscribed by three very firm facts. (1) The Constitution requires open trials. (2) Prosecution of spies or leakers often requires evidence the disclosure of which in open court would do more harm than the prosecutor's success

would do good. (3) Civil libertarians, not unjustly, are afraid of making mere disclosure of classified information a strict -- liability crime because information is often classified improperly.

Thus, it is not surprising the report can point the way to only marginal improvements in our ability to enforce laws safeguarding secrets. These improvements would be effected by conferring greater powers on judges to exclude certain evidence from espionage trials, and greater reliance on administrative sanctions to curb leaking by the government's present or former employees. Yet the former may well affect the fairness of trials, while the latter would surely provide for the non-judicial execution of penalties weightier than those meted out in most judicial proceedings. These may be excessive prices for such modest improvements.

A somewhat different line of analysis, however, can lead us to a solution at once much more efficacious against "disclose or dismiss," at least as respectful of civil liberties, and patently fairer than the solution advanced by the report. In brief: One need not alter the Sixth Amendment's guarantee of public trials, and one need not disclose classified information at public trials if the only question to be decided at such trials is whether the accused did or did not disclose classified information to unauthorized persons. But the question "did he unlawfully disclose" is logically independent of the one regarding the <u>effect</u> of the disclosure. Penalties need be

imposed only if it is determined that the disclosure caused or could cause harm to the United States. The question of harm done -- as distinguished from the questions of guilt and innocence and of motive -- could be tried in camera by a judge, with or without a cleared jury, and with cleared attorneys, without violating the letter or the spirit of the Sixth Amendment.

-- The two questions "did he do it" and "what harm did it do" are logically separate. Heretofore our judicial system has mixed them. Unless a statute is enacted to provide for their separate resolution, we will find no solution to the quandary "disclose or dismiss."

Did he do it?

It is useful to start from the fact that officials of the executive branch who classify information often do it erroneously and sometimes maliciously. Nevertheless, information does exist the disclosure of which would harm the country. Moreover, the people who work with it, no matter how imperfect their minds and motives, cannot help but be charged with the task of deciding which information deserves special protection and which does not. Their decision should not be final, but neither should the law regard it as merely one opinion among others. Were the law to give its judgment no special weight, the executive branch could

11

not lawfully keep reporters from TASS out of the Pentagon's war room.

Of course the executive branch's judgments on classification must be open to challenge in court. But, until such challenges are upheld, the executive must have the right to operate on a day-to-day basis as if its judgments were correct. That requires, at a minimum, that the judicial process be allowed to determine whether a given individual did or did not handle classified information in a manner deemed unlawful by the executive branch.

In recent years, the judiciary has not been able to make such determinations, because it has mixed the question "did he do it" with the question of whether the information involved was properly classified. The latter question is essential, but it is separate.

What harm did it do?

Civil libertarians are correct in stating that information is often improperly and sometimes maliciously classified, and that those who bring it into the public domain deserve praise. But no one disputes that some unauthorized disclosures are harmful. No one should object to determining whether and to what extent any particular disclosure was harmful.

72

We should object to accepting uncritically the intelligence agencies' own assessment of the harm done. Such assessments are the bases of the prosecution's case, and the chief targets for the defense. It follows therefore that an impartial court must decide between adversary presentations on the question of harm done.

But it does not follow that courts must decide the question of harm done in public. This question can and should be answered without any reference to the identity of the person(s) suspected of disclosing the classified information, or to their motives. The resolution of this question cannot in any way be considered the trial of a person. Therefore, the Sixth Amendment's guarantee of a public trial, which refers to trials of persons does not apply to this question.

There are several ways for the judicial system to decide such questions in camera. Grand juries routinely and secretly decide questions of fact, often examining evidence and arguments from varied sources. Perhaps major unauthorized disclosures of classified information could be brought before grand juries, which would issue their findings concerning the harm to be expected from the disclosure without even knowing the identity of any suspect(s). This would not constitute a secret trial because although the grand jury's decision would ultimately affect anyone found guilty

13

of disclosing the information in question, it would affect any such person equally. Its evaluation would prescind entirely from the accused's identity. The grand jury's assessment of harm done would be immune to the defense's challenges in an open trial for leaking or espionage. Indeed the question of harm done would be immaterial. Then, assuming such a trial resulted in conviction, the judge would turn to the grand jury's report to decide whether the defendant deserved a token sentence and contratulations for having served his country, or severe punishment for having endangered his fellow citizens, or any sentence in between.

One could object to the above procedure by maintaining that the interest of anyone accused of unlawful disclosure in the assessment of damage done is so great that no such assessment can be considered legally authoritative unless the defendant has had the opportunity to take part in the selection of the jury and in the arguments before it. A corollary of this objection is that courts may not give opinions outside the framework of "cases and controversies." These objections could be met by having the question of harm done decided in camera by the same jury which had tried the case of unlawful disclosure in open court, and by allowing the accused and his attorneys to compel and present whatever evidence they and the court deemed

relevant. Of course all parties to the proceedings would be sworn to secrecy and liable to severe penalties for violating it. Such a proceeding would not constitute a secret trial because, although the convict would have an interest in its outcome, the jury's decision on the harm done by the disclosure would depend not at all on what the convict had done, or his motives, or on his person. It would depend only on the qualities inherent in the information disclosed. These qualities would be on trial, not the person.

The Question of Harm

The question before us is how to punish those who harm their fellow Americans by unauthorized disclosures, and how to do so without infringing on the Constitution or civl liberties. The distinctions between leaks and espionage, between good and bad motives, between the release of substantive information and information regarding sources and methods are all of secondary importance. In fact, when disclosure cases from each of these different categories have come to trial, the proceedings have turned on one paramount question: "What harm did this do?" This is true even of cases under Section 798, U. S. Code (the statute protecting communications intelligence). And it seems reasonable

that this be so. Of course, the centrality of this question is the source of the legal quandary "disclose or dismiss."

Lately, attempts have been made to sidestep the question of harm done in order to make punishment of disclosures easier without recourse to an "official secrets act." The essence of these attempts has been to establish categories of disclosure which ipso facto result in harm to the United States. The release of substantive information may or may not do harm, while presumably the disclosure of intelligence sources and methods, as well as of intelligence operatives, is always harmful. Thus the proposals to make the disclosure of CIA employees, or of sources and methods, into strict liability crimes. But they will not work. No doubt disclosure of such information is harmful and should be punished. But why give these categories special attention and a higher likelihood of punishment and not to others (e.g., the location of SSBNs) the disclosure of which would be even more harmful? The only answer, that it is legally easier to do so, is unsatisfactory. The ruling criterion for punishment is, and must remain, harm.

Administrative Sanctions

Another attempt to handle the problem without recourse to strict liability for unlawful disclosure is reliance on administrative sanctions by agencies against offending employees or

against the pensions of former employees. But such sanctions are indefensible except as punishment for exposing the country to harm. Should any employee of the United States be punished administratively except for having done harm to his country? We rightly answer "no" because agencies' rules are not made for the agencies' heads' convenience, but for the good of the country.

Leaking by senior officials has become a part of our government's folkways -- a dangerous and unfair part. Senior officials can now punish junior ones very seriously by withdrawing their security clearances ostensibly for unauthorized disclosure of classified information, while they themselves disclose it without authorization but with impunity. Selective leaks of intelligence by senior officials is the most common and most dangerous means by which the CIA interferes in American politics. Today administrative sanctions are liable to the charge of arbitrariness. However, as we impose legal penalties upon leakers, we must not hinder the President, and senior officials designated by him, from wielding classified information, selectively and covertly as a weapon in the nation's arsenal. Ultimately, nothing can prevent a President from wielding such information to his partisian advantage except a public opinion that is well-informed and fairminded. But the law can control employees

11

of the United States, regardless of rank, who are not following the President's direct orders. If such an employee does harm to his country by leaking, even for the best motives, why shouldn't he be punished by the law? To put this from another perspective: Why should the legal system countenance the imposition of very heavy penalties (dismissal and loss of clearance for a career intelligence man are worse than jail) except for harm done to the United States? Does not the establishment of a non-judicial system for meting out such punishment mean a possible detour into corporativism -- a destination far more fearsome than an official secrets act?

Conclusion

In short, the Government may keep information out of the public domain only if its possession by our enemies would harm the United States. Now and again, Government officials will err, sometimes maliciously, in classifying information. But they must have the right to classify, and the fact of unlawful disclosure must be legally ascertainable. The key question of harm done -- on which punishment depends -- is both separate and not subject to the requirements for an open trial. That is because a trial of the question of harm done does not determine the guilt or innocence of any person, but rather the impersonal effect of an

action. Since the finding concerning this effect would bear upon the sentence imposed upon a person, that person ought to have the privilege of being present, of having counsel, of compelling witnesses, etc. But nothing in our Constitution, laws, or indeed in common sense, argues that these proceedings ought to be open. Parties to such proceedings must be held to secrecy, even as grand juries are.

It is immaterial whether the determination of harm done takes place before or after the trial of the person accused of unlawful disclosure. It is essential that this determination be made in secret -- so that it may be done with the benefit of all relevant information and without danger to the country. It is equally important that the determination be made judicially -- that is, by an impartial judge and jury, with adversary counsel -- for the sake of accuracy and of legal validity.

Soon the country will witness the attempt of our legal system to try Mr. Kampiles for allegedly selling the technical manual of the KH-11. Did he do it? That will be easy enough to prove or disprove. But his attorney will ask, legitimately, just how much harm the disclosure did. Any accounting of harm must weigh our knowledge of any countermeasures the Soviets may have taken since the disclosure, against the information on the

KH-11's targets provided by other sources. That kind of evaluation -- most relevant to the question of harm done -- simply cannot be discussed in public. So, if we hamstring our legal system by imprudently mixing two questions which are logically separate ("Did he do it?" and "What harm did it do?"). We will, irresponsibly, have to conclude we cannot try Mr. Kampiles. And if we can't try him, whom can we try?

The country could not accept imprudent adherence to unsound doctrine as an excuse for such irresponsibility.

This Committee should consider legislation to:

(1) establish stricter guidelines for classifying information as important to the nation's security.

(2) establish procedures for releasing classified information to the public.

(3) make the unauthorized disclosure of classified information a strict-liability crime, to be tried in open court with full constitutional guarantees.

(4) make punishment for the crime of unauthorized disclosure vary between purely nominal (e.g., one dollar fine) and heavy penalties, depending on the disclosed information's importance to the nation and to the harm to be reasonably expected from the disclosure.

80

(5) vest the right to determine harm done by the disclosure in the trial jury, meeting in camera, subject to security clearance and bound to secrecy. The attorneys would be similarly cleared and bound.

(6) ensure that the two questions be handled separately in the appeals process and that the question of harm done continue to be decided in camera.